

ABSTRACT

Call forwarding can be used to commit fraud or to evade security controls in inmate calling systems. Information from the Common Channel Signaling (CCS) network can be used to detect when a dialed number has been call forwarded and furthermore prevent the call forwarding event from occurring. It is possible to determine whether a dialed number has been call forwarded by setting up a call to that number with the Redirection Counter in the Initial Address Message set to the maximum value allowed in the signaling system being utilized (e.g., CCS7). If the terminating switch fails to set up the call even though the trunk is available, the assumption is made that the call is call forwarded. A second attempt is then made to set up the call a second time setting the Redirection Counter in the Initial Address Message to zero. If the terminating switch returns an Answer Complete Message indicating that the call has been successfully set up, then it has been demonstrated that the dialed number is call forwarded. This information can then be used to terminate the call attempt to the forwarded number, or alternatively, a variety of fraud prevention and/or fraud tracking processes can be initiated. Call forwarding events can be detected without the use of a telecommunications switch through which the call must pass.